Appl. No. 10/643,564
Amendment and Response dated March 31, 2008
Reply to Office Action of December 31, 2007

REMARKS

Claims 1, 3-11, and 15-28 were pending in the application at the time of examination.

Claims 1, 26, 27, and 28 are amended as detailed herein. Claim 4 is cancelled without prejudice.

Applicants submit the amendments are supported in the application as filed, and that no new matter has been added.

Applicants respectfully request reconsideration of the application.

Claims 1, 3, 5-11, and 15-28 are presented for examination.

Claim Objections

In the Office Action at page 2, the Examiner objected to Claims 27-28 stating:

> …these claims should refer to "the computer readable medium configured to store computer program code further comprising…" instead of to "the computer program product of claim 26 further comprising…."

The Examiner has required appropriate correction.

Applicants have amended Claims 27 and 28 to further recite "…the computer readable medium configured to store computer program code…" as required by the Examiner. Applicants submit Claims 27 and 28 as amended overcome the Examiner's objections.

Applicants respectfully request reconsideration and withdrawal of the objections to each of Claims 27 and 28.

Claim Rejections 35 USC 112

In the Office Action at page 3, the Examiner rejected Claims 4 and 27 under 35 USC 112, second paragraph as being indefinite. In particular, the Examiner stated the term "recently" "…is a relative term which renders the claims indefinite…."

Appl. No. 10/643,564
Amendment and Response dated March 31, 2008
Reply to Office Action of December 31, 2007

Applicants have cancelled Claim 4 thus rendering the rejection of Claim 4 moot.   Applicants have amended Claim 27 to delete the term "recently".   Applicants submit Claim 27 as amended overcomes the Examiner's rejection.

Applicants respectfully request reconsideration and withdrawal of the 35 USC 112 rejections of each of Claims 4 and 27.

Rejections under 35 U.S.C. 103(a): Pak/Hoepers

In the Office Action at page 3, the Examiner rejected Claims 1, 3-7 and 26-28 under 35 U.S.C. 103(a) as being unpatentable over Pak et al., USPN 7,080,408 (hereinafter Pak) further in view of Hoepers et al., "Honeynets Applied to the CSIRT Scenario" (hereinafter Hoepers).

Claims 1, 3-7 and 26-28 are not obvious over Pak and Hoepers

Claim 1

Applicants have amended Claim 1.

With regard to independent Claim 1, in the Office Action at pages 3-4, the Examiner states:

> Pak et al. substantially teach a method/computer program product comprising a computer readable medium configured to store code, the method/computer program product comprising: comparing outbound traffic on a host computer system to inbound traffic on the host computer system, wherein the inbound traffic is received on the host computer system from a source external to the host computer system (col. 5, lines 3-28); and determining if malicious code is detected on the host computer system based on the comparing (col. 5, lines 28-30); when malicious code is detected, providing a notification of the malicious code detection (col. 7, line 4-12).
> Not explicitly disclosed is wherein the outbound traffic is generated on the host computer system for transmission from the host computer system to a

Appl. No. 10/643,564
Amendment and Response dated March 31, 2008
Reply to Office Action of December 31, 2007

destination external to the host computer system.
However, Hoepers et al. teach that outgoing traffic
generated on a host machine which are not in response
to an incoming packet received are captured and an
alert for interception of malicious traffic is
generated. Therefore, it would have been obvious to a
person in the art at the time the invention was made
to modify the method disclosed in Pak et al. to
compare the outgoing traffic to determine whether or
not it is in response to incoming/received traffic in
order to create an alert when the outgoing traffic is
generated on the host machine is not in response to
any of the received/incoming traffic. This
modification would have been obvious because a person
having ordinary skill in the art, a the time the
invention was made, would have been motivated to do so
since Hoepers et al. suggest that generating an alert
for outgoing traffic generated without being a
response to incoming traffic will lessen the impact
that malicious traffic has on a network on page 5,
section 2.4.1, number 1.

Applicants respectfully submit Pak does not describe or
suggest at least **comparing at least a portion of outbound
traffic on a host computer system to at least a portion of
inbound traffic on the host computer system**, wherein the inbound
traffic is received on the host computer system from a source
external to the host computer system, and wherein the outbound
traffic is generated on the host computer system for
transmission from the host computer system to a destination
external to the host computer system, and further **wherein the at
least a portion of the outbound traffic is subsequent in time to
the at least a portion of the inbound traffic**; and **determining
if malicious code is detected on the host computer system based
on the comparing**. (emphasis added)

For example, Pak at col. 4, lines 52-63 describes:

As shown, network communications are received in
operation 402, and are scanned for known malicious
code in operation 404. In operation 406, a
determination is made as to whether known malicious

Appl. No. 10/643,564
Amendment and Response dated March 31, 2008
Reply to Office Action of December 31, 2007

code has been detected. If known malicious code is detected, the data is cleaned in operation 408. The cleaning disables the malicious code such as by removing or recoding the malicious code.

With continued reference to Fig. 4, **if no known malicious code is detected, heuristics associated with the network communications are identified in operation 410 and monitored in operation 412.** (emphasis added)

Pak at col. 5, lines 3-28 additionally describes:

The determination as to whether the network communications contains potentially malicious content is preferably based on heuristics. Any suitable type of heuristic can be used.

According to one heuristic, **a histogram of content (attachments, subject line contents, etc.) is generated over a period of time. The histogram is analyzed to determine if multiple copies are being sent. Content can then be identified as potentially malicious when, for a given period of time, the number of similar or identical instances of the content in the network communications that pass through the network is greater than a predetermined value.** For example, when the network communications include electronic mail messages, an electronic mail message can be identified as having potentially malicious content when a number of messages having an identical subject line and/or attachment passing through the network for a given period of time is greater than a predetermined value. This helps prevent the spread of malicious content such as mass-mailer viruses and worms. As an example of use, suppose 100 copies of "Attachment A" have been received, scanned and delivered in the last 10 minutes. This may merely be SPAM, or it may be a mass mailing initiated by malicious code. Because the number of copies is above a prespecified threshold of 20 identical attachments per 10 minute period, further communications with these attachments are quarantined in a quarantine directory. (emphasis added)

Thus, Applicants submit Pak first scans an incoming communication for known malicious code, and then if no malicious code is found in the incoming communication based on the scan, Pak then describes that a histogram of content is generated over a time period and the histogram is then analyzed to

Appl. No. 10/643,564
Amendment and Response dated March 31, 2008
Reply to Office Action of December 31, 2007

determine if multiple copies are being sent. When a further communication of the type collected by the histogram exceeds a prespecified threshold, the further communication of that type can be quarantined.

Thus, Applicants submit Pak fails to describe or suggest comparing at least a portion of outbound traffic on a host computer system to at least a portion of inbound traffic; rather, Pak, after a non-indicative malicious code scan, develops a histogram of a same type of communication, for example, a received communication, and compares a further communication of the same type against a prespecified threshold.

Additionally, Pak fails to describe or suggest that the further communication is inbound traffic received on the host computer system from a source external to the host computer system, and that it is being compared to outbound traffic generated on the host computer system for transmission from the host computer system to a destination external to the host computer system. Accordingly, Pak thus also fails to describe or suggest that the at least a portion of the outbound traffic is subsequent in time to the at least a portion of the inbound traffic. Further, Pak fails to describe determining if malicious code is detected on the host computer system based on the comparing.

Hoepers at page 5, section 2.4.1, number 1 describes:

1.   Outgoing traffic

A script using tcdump, running in the IDS machine, filters the captured data. Any outgoing packet originating from the Honeynet, that is not in response to an incoming packet, generates an alert. All alerts are grouped and sent by email periodically.

Applicants submit the above reference to Hoepers describes that **any** outgoing packet from the Honeynet not in response to an incoming packet generates an alert, and thus the reference fails to correct the above deficiencies of Pak.

Appl. No. 10/643,564
Amendment and Response dated March 31, 2008
Reply to Office Action of December 31, 2007

Based on the above remarks, Applicants respectfully submit Pak and Hoepers fail to support an obviousness rejection of Claim 1. Claims 1, 3, 5-11 depend from Claim 1, and thus for at least the same reasons as Claim 1, Claims 3 and 5-11 are also not obvious. Claim 4 was cancelled.

Applicants respectfully request reconsideration and withdrawal of the 35 U.S.C. 103(a) rejections of each of Claims 1 and 3-7.

Claim 26

Claim 26 was amended similar to Claim 1. Accordingly, Applicants respectfully submit that for at least the same reasons earlier presented with respect to the 103(a) rejection of Claim 1, Pak and Hoepers also fail to support an obviousness rejection of Claim 26. Claims 27-28 depend from Claim 26, and thus for at least the same reasons as Claim 26, Claims 27-28 are also not obvious.

Applicants respectfully request reconsideration and withdrawal of the 35 U.S.C. 103(a) rejections of each of Claims 26-28.

Rejections under 35 U.S.C. 103(a): Hoepers/Chesla

In the Office Action at page 6, the Examiner rejected Claims 15-25 under 35 U.S.C. 103(a) as being unpatentable over Chesla et al., US Pub. No. 2004/0250124 (hereinafter Chesla) and further in view of Hoepers.

Claims 15-25 are not obvious over Chesla and Hoepers

Claims 15-19

Applicants respectfully traverse the obviousness rejections of each of Claims 15-19.

Appl. No. 10/643,564
Amendment and Response dated March 31, 2008
Reply to Office Action of December 31, 2007

In the Office Action at pages 6-7, the Examiner states:

> Chesla et al. substantially teach a method comprising: intercepting inbound traffic on a host computer system, wherein the inbound traffic is received on the host computer system from a source external to the host computer system (par. 121); copying the inbound traffic to an inbound traffic memory area, the copying the inbound traffic generating copied inbound traffic (par. 365-370); releasing the inbound traffic (par. 353-355); intercepting the outbound traffic on the host computer system (par. 149); copying the outbound traffic to an outbound traffic memory area, the copying the outbound traffic generating copied outbound traffic (par. 300); releasing the outbound traffic (par. 353-355); comparing at least a portion of the copied inbound traffic with at least a portion of the copied outbound traffic (par. 137); and if malicious code is detected, providing a notification of the malicious code detection (par. 435).

Applicants respectfully submit that the references to Chesla relied on by the Examiner fail to teach or suggest at least comparing at least a portion of the **copied inbound traffic** with at least a portion of the **copied outbound traffic**.

For example, the citation to Chesla at par. 137 describes in part:

> On the other hand, if the network flood controller determined at step 112 that the filtering was effective, i.e., the degree of the attack decreased as the result of filtering, the controller reacts to this positive feedback by increasing the filtering period and continuing to monitor the attack, at an attack monitoring step 118. In order to determine whether the attack is continuing, **the controller directs FIS module 62 to evaluate both unfiltered traffic from WAS 26 and filtered traffic from filtering module 70. The level of attack in both of these streams is compared**, at an attack stop check step 120. If both streams are evaluated as not containing an attack, the controller directs the

Appl. No. 10/643,564
Amendment and Response dated March 31, 2008
Reply to Office Action of December 31, 2007

filtering module to discontinue filtering, at a stop
filtering step 122, and the controller resumes
statistics collection at step 100 and attack
monitoring at step 101…. (emphasis added)

Applicants submit that the above reference to Chesla is
excerpted from a description of FIG. 3 and at most describes a
comparison of filtered **incoming traffic** and unfiltered **incoming
traffic**. More particularly, Applicants submit: the "unfiltered
traffic from WAN 26" monitored by FIS module 62 is **incoming
traffic** from WAN 26 (see FIG. 2 of Chesla showing flow of
incoming traffic from WAN 26); and, that the "filtered traffic
from filtering module 70" is **incoming traffic** that has been
filtered by filtering module 70 (see Chesla, page 8, par. 135:
"filtering module 70 filters incoming traffic, at a filtering
step 110"). Thus, Applicants submit the references to Chesla
relied on by the Examiner fail to teach or suggest at least
**comparing at least a portion of the <u>copied inbound traffic</u> with
at least a portion of the <u>copied outbound traffic</u>**.

The reference to Hoepers relied on by the Examiner at page
5, section 2.4.1, number 1, earlier discussed with reference to
the obviousness rejection of Claim 1, fails to correct the above
deficiencies of Chesla.

Based on the above remarks, Applicants respectfully submit
Chesla and Hoepers fail to support an obviousness rejection of
Claim 15. Claims 16-19 depend from Claim 15, and thus for at
least the same reasons as Claim 15, Claims 16-19 are also not
obvious.

Applicants respectfully request reconsideration and
withdrawal of the 35 U.S.C. 103(a) rejections of each of Claims
15-19.

GUNNISON, McKAY &
HODGSON, L.L.P.
Garden West Office Plaza
1900 Garden Road, Suite 220
Monterey, CA 93940
(831) 655-0880
Fax (831) 655-0888

Appl. No. 10/643,564
Amendment and Response dated March 31, 2008
Reply to Office Action of December 31, 2007

Claims 20-25

Applicants respectfully traverse the obviousness rejections of each of Claims 20-25.

Applicants respectfully submit that for at least the same reasons earlier presented with respect to the 103(a) rejection of Claim 15, Chesla and Hoepers also fail to support an obviousness rejection of Claim 20. Claims 21-25 depend from Claim 20, and thus for at least the same reasons as Claim 20, Claims 21-25 are also not obvious.

Applicants respectfully request reconsideration and withdrawal of the 35 U.S.C. 103(a) rejections of each of Claims 20-25.

Rejections under 35 U.S.C. 103(a): Pak/Hoepers/Chesla

In the Office Action at page 11, the Examiner rejected Claims 8-11 under 35 U.S.C. 103(a) as being unpatentable over Pak and Hoepers as applied to Claim 1, and further in view of Chesla.

Claims 8-11 are not obvious

Applicants respectfully traverse the obviousness rejections of each of Claims 8-11.

Claims 8-11 depend from Claim 1. Applicants respectfully submit that for at least the reasons earlier presented with respect to the 103(a) rejection of Claim 1, the cited references to Pak and Hoepers fail to support and obviousness rejection of Claim 1. Additionally, Applicants respectfully submit that for at least the reasons earlier presented with respect to the 103(a) rejection of Claim 15, the cited references to Chesla fail to correct the deficiencies of Pak and Hoepers.

Indeed, the Examiner has not asserted the combination of Pak/Hoepers/Chesla as teaching or suggesting Claim 1. Thus, on

Appl. No. 10/643,564
Amendment and Response dated March 31, 2008
Reply to Office Action of December 31, 2007

this basis alone, Claims 8-11 which depend from Claim 1 are not obvious over the combination of Pak, Hoepers, and Chesla.

Accordingly, Applicants submit Pak and Hoepers and Chesla, alone or in combination, fail to support an obviousness rejection of Claim 1. Claims 8-11 depend from Claim 1, and thus for at least the same reasons as Claim 1, Claims 8-11 are also not obvious.

Applicants respectfully request reconsideration and withdrawal of the 35 U.S.C. 103(a) rejections of each of Claims 8-11.

Conclusion

Claims 1, 3, 5-11, and 15-28 remain in the application. For the foregoing reasons, Applicants respectfully request allowance of all pending claims. If the Examiner has any questions relating to the above, the Examiner is respectfully requested to telephone the undersigned Attorney for Applicant(s).

Request for Examiner Interview

Should the Examiner be of the opinion that this amendment does not place the Application in a condition for allowance, Applicants respectfully request an Examiner interview prior to issuance of the next communication from the USPTO to expedite prosecution.

Respectfully submitted,

Lisa A. Norris
Attorney for Applicant(s)
Reg. No. 44,976
Tel.: (831) 655-0880